A Multi-Dimensional Mean Failure Cost Model to Enhance Security of Cloud Computing Systems

Mouna Jouini, Laboratoire SOIE, Institut Supérieur de Gestion, Tunis, Tunisia
Latifa Ben Arfa Rabai, Laboratoire SOIE, Institut Supérieur de Gestion, Tunis, Tunisia

ABSTRACT
Cloud computing technology is a relatively new concept of offering reliable and virtualized resources, software and hardware on demand to users. It presents a new technology to deliver computing resources as a service. It allows several benefits for example services on demand, provisioning, shared resources and pay per use and suffers from several challenges. In fact, security presents a major obstacle in cloud computing adoption. In this paper, the authors will deal with security problems in cloud computing systems and estimate security breaches using a quantitative security risk assessment model. Finally, the authors use this quantitative model to solve these problems in cloud environments.

KEYWORDS
Cloud Computing, Countermeasures, Multidimensional Mean Failure Cost (M²FC), Security Issues, Security Quantification, Threats

1. INTRODUCTION
Cloud Computing (CC) is an emerging technology which recently has shown significant attention lately in the world. It has several advantages like pay per use, resource pooling and scalability. The National Institute of Standard and Technology (NIST) definition defines cloud computing as a paradigm for enabling useful, on-demand network access to a shared pool of configurable computing resources (Mell & Grance, 2010; Shrivastava & Bhilare, 2015). It offers several services presented in three models: Software as Service (SaaS), Platform as Service (PaaS), and Infrastructure as Service (IaaS). Software as Service (SaaS) provides applications or software to end users, Platform as Service (PaaS) provides access to platforms and Infrastructure as Service (IaaS) offers processing storage service.

Cloud Computing offers many advantages. However, the biggest challenge in cloud computing is the security and privacy problems caused by its multi-tenancy nature and the outsourcing of infrastructure, sensitive data and critical applications which causes serious consequences (Sun, Zhang, Xiong, & Zhu, 2014; Kushwah & Saxena, 2013; Kushwah & Saxena, 2013; Youssef & Alageel, 2012; Aljawarneh & Bani Yassein, 2016; Mell & Grance, 2010; Ben Arfa Rabai, Jouini, Ben Aissa & Mili, 2012; Jouini, Ben Arfa Rabai, Ben Aissa & Mili, 2012; Ben Arfa Rabai, Jouini, Ben Aissa & Mili, 2013; Jouini, Ben Arfa Rabai & Ben Aissa, 2014; Sampathkumar, 2015; Shrivastava & Bhilare, 2015; Jakimoski, 2016). In fact, According to survey conducted by International Data Group (IDG) enterprise in 2014 (IDG Cloud Computing Survey, 2014), security is deeply the top concern for cloud computing. In fact, up from 61% in 2014, and higher among finance organizations (78%), 67% of organizations have concerns about the security of Cloud Computing solutions. The additional challenges are not
even on the same playing field for tech decision-makers; only 43% are concerned with integration,
followed by the ability of cloud solutions to meet enterprise and/or industry standards (35%) (IDG
Cloud Computing Survey, 2014). Given their high security concerns, organizations are integrating
strategies and tools (like cloud management and monitoring tools, and cloud security management
tools) to lessen these challenges over the next 12 months.

In this paper, we show the use of a quantitative security risk analysis model to estimate security
breaches for Cloud Computing systems by considering new threats perspectives. Then, we will
show how to solve security problems in Cloud Computing systems using a quantitative security risk
assessment model. We aim to present a generic framework that evaluates firstly cloud security by
identifying unique security requirements, secondly to identify architectural components affected by
this risk, thirdly to make out security threats that damage these components and finally to attempt to
present viable solutions that eliminate these potential threats.

The remainder of this paper is organized as follows. Section 2 presents related work. Section
3 presents security challenges in Cloud Computing environments. Section 4 defines the Multi-
dimensional Mean Failure Cost model (M2FC) and illustrates its use to quantify security risk on a
practical case study. Section 5 presents our security framework that solves security problems in CC
in a quantitative way. Finally, conclusions and a direction for future work are given in section 6.

2. RELATED WORK

Literature review was illustrated that there are several works that studied cloud computing security
concerns (Sun, Zhang, Xiong, & Zhu, 2014; Kushwah & Saxena, 2013; Kushwah & Saxena, 2013;
Youssef & Alageel, 2012; Aljawarneh & Bani Yassein, 2016; Jakimoski, 2016; Hassan Hussein &
Khalid, 2016). All works provide a qualitative discussion of security-related issues in CC environments
submitting a quick analysis and survey of security issues. However, in this article, we develop and
deploy a qualitative security management framework on CC environment by proposing some security
strategies (countermeasures).

Sun et al. present in (Sun, Zhang, Xiong, & Zhu, 2014) a review of security and privacy concerns
in Cloud Computing systems as cloud data are stored in different locations in the world. They assess
as well various security challenges from both software and hardware views for protecting data in
the cloud in order to ameliorate security and privacy for customer’s data. In addition, authors present
a survey of data security and privacy techniques for data protection to attain highest level of data
security in the cloud.

Kushwah & Saxena highlighted CC security issues and especially data privacy and confidentiality
due to customers’ data and application migration to the cloud (Kushwah & Saxena, 2013). It fact, the
article consider that data migration to a Cloud Computing environment has many ways to exercise
risk and has several serious impact to the integrity, confidentiality and auditability of the system.
The paper presents the importance and motivation of security in the migration of legacy systems and
carries out an approach related to security in migration processes to cloud with the aim of finding
the needs, concerns, requirements, aspects, opportunities and benefits of security in the migration
process of legacy systems. The approach for secure cloud data migration process uses encryption and
decryption keys techniques (a set of attributes to design user’s decryption keys and to encrypt simple
text messages. Decryption occurs when a match occurs between the attributes held by the entity (in
their Decryption key) and the attributes used to construct a simple text.)

Alemu & Omer proposed a Cloud Computing Security Framework for Banking Industry as
this new technology is adopted in several areas in the world (Alemu & Omer, 2014). The framework
incorporates major components that address security, privacy, legal and compliance and regulatory
issues for cloud systems and aims to preserve the availability, integrity, and confidentiality of an
organization’s information. The framework is inspired from the architects view of SABSA model
(Sherwood, Clark, & Lynas, 2009) that it defines principles and fundamental concepts that guide
Development of a Complex Geospatial/RF Design Model in Support of Service Volume Engineering Design

Global Heterogeneity in the Emerging M-Commerce Landscape